AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An encryption method for dividing a first plaintext bit stream of length 2n into first and second sub-bit streams of length n, dividing a second plaintext bit stream of length 2n into third and fourth sub-bit streams of length n, and generating a ciphertext bit stream of length 2n from the first, second, third and fourth sub-bit streams using 2-rounds of encryption, the method comprising the steps of:

performing a first-round of encryption by encrypting the received the first and second sub-bit streams with predetermined first encryption codes an odd number of times, and outputting the second ciphertext bit stream ~~having been once more~~ encrypted again with a predetermined time delay right after the first ciphertext bit streams of length n are outputted;

generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream at the same time of performing encryption of the second ciphertext bit stream;

generating a second operated ciphertext bit stream by performing a logical exclusive-OR operation on the second ciphertext bit stream and the fourth sub-bit stream; and

performing a second-round of encryption by encrypting the received ~~the~~ first operated ciphertext bit stream and the second operated ciphertext bit stream, ~~having~~comprising the predetermined time delay, with predetermined second encryption codes an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams of length n after ~~once more~~ encrypting the first operated ciphertext bit stream again with predetermined second encryption codes.

2. (Currently Amended) The encryption apparatus of claim 1, wherein the predetermined ~~second~~ first encryption codes comprises at least one of $KO_{1,1}$, $KO_{1,2}$, $KO_{1,3}$, $KI_{1,1}$, $KI_{1,2}$, and $KI_{1,3}$.

3. (Currently Amended) The encryption apparatus of claim 1, wherein the ~~first~~ predetermined second encryption codes comprises at least one of $KO_{2,1}$, $KO_{2,2}$, $KO_{2,3}$, $KI_{2,1}$, $KI_{2,2}$, and $KI_{2,3}$.

4. (Currently Amended) The encryption method of claim 2, wherein the first-round encryption step comprises the steps of:

generating a first signal by performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code $KO_{1,1}$ to provide a first exclusive-OR operated bitstream, encrypting the first exclusive-OR-operated bit stream with the first encryption code $KI_{1,1}$ to provide a first encrypted signal, and performing a logical exclusive-OR operation on the first encrypted signal and the second sub-bit stream delayed by time required for the encryption;

generating the first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second sub-bit stream and the first encryption code $KO_{1,2}$, to provide a second exclusive-OR operated bitstream[[,]] encrypting the second exclusive-OR-operated bit stream with the first encryption code $KI_{1,2}$, to provide a second encrypted signal, and performing a logical exclusive-OR-operation on the second encrypted signal and the first signal;

generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first signal and the first encryption code $KO_{1,3}$ to provide a third exclusive-OR operated bitstream, encrypting the third exclusive-OR-operated bit stream with the first encryption code $KI_{1,3}$, and performing a logical exclusive-OR-operation on the encrypted signal with the first sub-bit stream delayed by time required for the encryption.

5. (Currently Amended) The encryption method of claim 3, wherein the second-round encryption step comprises the steps of:

generating a second signal by performing a logical exclusive-OR-operation on the first operated ciphertext bit stream and the second encryption code $KO_{2,1}$ to provide a fourth

exclusive-OR operated bitstream, encrypting the fourth exclusive-OR-operated bit stream with the second encryption code $KI_{2,1}$ to provide a third encrypted signal, performing a logical exclusive-OR-operation on the third encrypted signal and the second operated ciphertext bit stream to provide a fifth exclusive-OR operated bitstream;

generating the third operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second operated ciphertext bit stream and the second encryption code $KO_{2,2}$, encrypting the fifth exclusive-OR-operated bit stream with the second encryption code $KI_{2,2}$ to provide a fourth encrypted signal, and performing a logical exclusive-OR-operation on the fifth encrypted signal and the second signal delayed by time required for the encryption; and

generating the fourth ciphertext bit stream by performing a logical exclusive-OR-operation on the second signal and the second encryption code $KO_{2,3}$ encrypting the sixth exclusive-OR-operated bit stream with the second encryption code $KI_{2,3}$, and performing a logical exclusive-OR-operation on the encrypted signal with the third operated ciphertext bit stream.

6. (Original) The encryption method of claim 5, wherein each of the encryptions includes first and second sub-encryptions, and outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal.

7. (Original) The encryption method of claim 5, wherein a 16-bit input bit stream is divided into a 9-bit stream and a 7-bit stream, a 9-bit ciphertext bit stream is generated from the 9-bit stream using a first equation, and a 7-bit ciphertext bit stream is generated from the 7-bit stream using a second equation in each of the sub-encryptions, wherein said first equation comprises

y0 = (x0x2)⊕x3⊕(x2x5)⊕(x5x6)⊕(x0x7)⊕(x1x7)⊕(x2x7)⊕(x4x8)⊕(x5x8)⊕(x7x8)⊕'1';
y1 = x1⊕(x0x1)⊕(x2x3)⊕(x0x4)⊕(x1x4)⊕(x0x5)⊕(x3x5)⊕x6⊕(x1x7)⊕(x2x7)⊕(x5x8)⊕'1';
y2 = x1⊕(x0x3)⊕(x3x4)⊕(x0x5)⊕(x2x6)⊕(x3x6)⊕(x5x6)⊕(x4x7)⊕(x5x7)⊕(x6x7)⊕x8⊕(x0x8)⊕'1';
y3 = x0⊕(x1x2)⊕(x0x3)⊕(x2x4)⊕x5⊕(x0x6)⊕(x1x6)⊕(x4x7)⊕(x0x8)⊕(x1x8)⊕(x7x8);
y4 = (x0x1)⊕(x1x3)⊕x4⊕(x0x5)⊕(x3x6)⊕(x0x7)⊕(x6x7)⊕(x1x8)⊕(x2x8)⊕(x3x8);
y5 = x2⊕(x1x4)⊕(x4x5)⊕(x0x6)⊕(x1x6)⊕(x3x7)⊕(x4x7)⊕(x6x7)⊕(x5x8)⊕(x6x8)⊕(x7x8)⊕'1';
y6 = x0⊕(x2x3)⊕(x1x5)⊕(x2x5)⊕(x4x5)⊕(x3x6)⊕(x4x6)⊕(x5x6)⊕x7⊕(x1x8)⊕(x3x8)⊕(x5x8)⊕(x7x8);
y7 = (x0x1)⊕(x0x2)⊕(x1x2)⊕x3⊕(x0x3)⊕(x2x3)⊕(x4x5)⊕(x2x6)⊕(x3x6)⊕(x2x7)⊕(x5x7)⊕x8⊕'1';
y8 = (x0x1)⊕x2⊕(x1x2)⊕(x3x4)⊕(x1x5)⊕(x2x5)⊕(x1x6)⊕(x4x6)⊕x7⊕(x2x8)⊕(x3x8);

and said second equation comprises

y0=(x1x3)⊕x4⊕(x0x1x4)⊕x5⊕(x2x5)⊕(x3x4x5)⊕x6⊕(x0x6)⊕(x1x5)⊕(x3x5)⊕(x2x4x6)⊕(x1x5x6)⊕(x4x5x6);
y1=(x0x4)⊕(x0x4)⊕(x2x4)⊕x5⊕(x1x2x5)⊕(x0x3x5)⊕x6⊕(x0x2x6)⊕(x3x6)⊕(x4x5x6)⊕'1';
y2=x0⊕(x0x3)⊕(x2x3)⊕(x1x2x4)⊕(x0x3x4)⊕(x1x5)⊕(x0x2x5)⊕(x0x6)⊕(x0x4x6)⊕(x2x6)⊕(x4x6)⊕'1';
y3=x1⊕(x0x1x2)⊕(x1x4)⊕(x3x4)⊕(x0x5)⊕(x0x4x5)⊕(x2x3x5)⊕(x1x4x5)⊕(x2x6)⊕(x1x3x6);
y4=(x0x2)⊕x3⊕(x1x3)⊕(x0x1x4)⊕(x0x1x4)⊕(x2x3x4)⊕(x0x5)⊕(x1x3x5)⊕(x0x4x5)⊕(x1x6)⊕(x3x6)⊕(x0x3x6)⊕(x5x6)⊕'1';
y5=x2⊕(x0x2)⊕(x0x3)⊕(x1x2x3)⊕(x0x2x4)⊕(x0x5)⊕(x2x5)⊕(x1x5)⊕(x1x6)⊕(x1x2x6)⊕(x0x3x6)⊕(x3x4x6)⊕(x2x5x6)⊕'1';
y6=(x1x2)⊕(x0x1x3)⊕(x0x4)⊕(x1x5)⊕(x3x5)⊕x6⊕(x0x1x6)⊕(x2x3x6)⊕(x1x4x6)⊕(x3x5x6);

8. (Currently Amended) An encryption apparatus for dividing a first plaintext bit stream of length 2n into first and second sub-bit streams of length n, dividing a second plaintext bit stream of length 2n into third and fourth sub-bit streams of length n, and generating a ciphertext bit stream of length 2n from the first, second, third and fourth sub-bit streams using 2-rounds of encryption, the apparatus comprising:

a first ciphering unit for receiving the first and second sub-bit streams, and generating first and second ciphertext bit streams of length n by encrypting the first and second sub-bit streams with predetermined first encryption codes $KO_{1,1}$, $KO_{1,2}$, $KO_{1,3}$, $KI_{1,1}$, $KI_{1,2}$, and $KI_{1,3}$ an odd number of times, and the second ciphertext bit stream ~~having been once more~~

encrypted again with a predetermined time delay after the first ciphertext bit streams of length n are outputted;

an operating unit for generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream at the same time of performing the first-round of encryption, and generating a second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second ciphertext bit stream with the fourth sub-bit stream; and

a second ciphering unit for receiving the first operated ciphertext bit stream and the second operated ciphertext bit stream ~~having~~ comprising the predetermined time delay, generating third and fourth ciphertext bit streams of length n by encrypting the first operated ciphertext bit stream and the second operated ciphertext bit stream with predetermined second encryption codes $KO_{2,1}$, $KO_{2,2}$, $KO_{2,3}$, $KI_{2,1}$, $KI_{2,2}$, and $KI_{2,3}$ an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams after ~~once more~~ encrypting the first operated ciphertext bit stream again with predetermined second encryption codes.

9. (Currently Amended) The encryption apparatus of claim 8, wherein the first ciphering unit comprises:

a first block ~~having~~ comprising a first exclusive-OR operator for performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code $KO_{1,1}$, a first sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code $KI_{1,1}$, and a second exclusive-OR operator for generating a first signal by performing a logical exclusive-OR operation on the encrypted signal with the second sub-bit stream being delayed to provide time for the encryption;

a second block ~~having~~ comprising a third exclusive-OR operator for performing a logical exclusive-OR operation on the second sub-bit stream and the first encryption code $KO_{1,2}$, a second sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code $KI_{1,2}$, and a fourth exclusive-OR operator for generating the first operated

ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the first signal; and

a third block ~~having~~ comprising a fifth exclusive-OR operator for performing a logical exclusive-OR operation on the first signal and the first encryption code $KO_{1,3}$, a third sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code $KI_{1,3}$, and a sixth exclusive-OR operator for generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal and the first sub-bit stream delayed by time required for the encryption.

10. (Currently Amended) The encryption apparatus of claim 8, wherein the second ciphering unit comprises:

a fourth block ~~having~~ comprising a seventh exclusive-OR operator for exclusive-OR-operating the first operated ciphertext bit stream with the second encryption code $KO_{2,1}$, a fourth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption code $KI_{2,1}$, and an eighth exclusive-OR operator for generating a second signal by performing a logical exclusive-OR-operation on the encrypted signal and the second operated ciphertext bit stream;

a fifth block ~~having~~ comprising a ninth exclusive-OR operator for exclusive-OR-operating the second operated ciphertext bit stream with the second encryption code $KO_{2,2}$, a fifth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption code $KI_{2,2}$, and a tenth exclusive-OR operator for generating the third ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal and the second signal delayed by time required for the encryption; and

a sixth ~~bock having~~ block comprising an eleventh exclusive-OR operator for performing a logical exclusive-OR operation on the second signal with the second encryption code $KO_{2,3}$, a sixth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption code $KI_{2,3}$, and a twelfth exclusive-OR operator for generating the fourth

ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the third ciphertext bit stream.

11. (Currently Amended) The encryption apparatus of claim 10, wherein each of the first to sixth sub-ciphers includes first and second sub-ciphering units, and a register for storing the outputs of the first and second sub-ciphering units and simultaneously ~~retrieve~~ retrieving the outputs according to an external clock signal.

12. (Original) The encryption apparatus of claim 11, wherein each of the first and second sub-ciphering units divides a 16-bit input bit stream into a 9-bit stream and a 7-bit stream, and generates a 9-bit ciphertext bit stream from the 9-bit stream using a third equation, and a 7-bit ciphertext bit stream from the 7-bit stream using a fourth equation, said third equation comprising

y0 = (x0x2)⊕x3⊕(x2x5)⊕(x5x6)⊕(x0x7)⊕(x1x7)⊕(x2x7)⊕(x4x8)⊕(x5x8)⊕(x7x8)⊕'1';
y1 = x1⊕(x0x1)⊕(x2x3)⊕(x0x4)⊕(x1x4)⊕(x0x5)⊕(x3x5)⊕x6⊕(x1x7)⊕(x2x7)⊕(x5x8)⊕'1';
y2 = x1⊕(x0x3)⊕(x3x4)⊕(x0x5)⊕(x2x6)⊕(x3x6)⊕(x5x6)⊕(x4x7)⊕(x5x7)⊕(x6x7)⊕x8⊕(x0x8)⊕'1';
y3 = x0⊕(x1x2)⊕(x0x3)⊕(x2x4)⊕x5⊕(x0x6)⊕(x1x6)⊕(x4x7)⊕(x0x8)⊕(x1x8)⊕(x7x8);
y4 = (x0x1)⊕(x1x3)⊕x4⊕(x0x5)⊕(x3x6)⊕(x0x7)⊕(x6x7)⊕(x1x8)⊕(x2x8)⊕(x3x8);
y5 = x2⊕(x1x4)⊕(x4x5)⊕(x0x6)⊕(x1x6)⊕(x3x7)⊕(x4x7)⊕(x6x7)⊕(x5x8)⊕(x6x8)⊕(x7x8)⊕'1';
y6 = x0⊕(x2x3)⊕(x1x5)⊕(x2x5)⊕(x4x5)⊕(x3x6)⊕(x4x6)⊕(x5x6)⊕x7⊕(x1x8)⊕(x3x8)⊕(x5x8)⊕(x7x8);
y7 = (x0x1)⊕(x0x2)⊕(x1x2)⊕x3⊕(x0x3)⊕(x2x3)⊕(x4x5)⊕(x2x6)⊕(x3x6)⊕(x2x7)⊕(x5x7)⊕x8⊕'1';
y8 = (x0x1)⊕x2⊕(x1x2)⊕(x3x4)⊕(x1x5)⊕(x2x5)⊕(x1x6)⊕(x4x6)⊕x7⊕(x2x8)⊕(x3x8);

and said fourth equation comprising